WHEN IS -1 A SQUARE MODULO PRIMES?

KEITH CONRAD

When p is an odd prime, there are two natural ways to pair off nonzero numbers mod p: pair each number with its multiplicative inverse or with its additive inverse. Using both of these ideas will lead to a proof of the pattern for when -1 mod p is a square:

$$-1 \equiv \square \bmod p \iff p = 2 \text{ or } p \equiv 1 \bmod 4.$$

Theorem 1 (Wilson)**.** *For any prime p, $(p-1)! \equiv -1 \bmod p$.*

Proof. In the product

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)$$

on the right side the factors run through all the nonzero numbers mod p. For each k from 1 to $p-1$, there's a k' from 1 to $p-1$ such that $kk' \equiv 1 \bmod p$. Let's pair together multiplicative inverses mod p. As long as $k' \neq k$, both k and k' are in the product for $(p-1)!$ and they cancel each other mod p (each is the other's multiplicative inverse). The only time there isn't cancellation of k by k' in $(p-1)!$ mod p is when $k' = k$, which means $k^2 \equiv 1 \bmod p$. That is the same as $k \equiv \pm 1 \bmod p$, so $k = 1$ and $k = p-1$. Therefore

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \bmod p.$$

□

Example 2. When $p = 7$,

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6,$$

where we collected inverse pairs mod 7: 2 and 4, and 3 and 5. Reducing the product modulo 7, terms cancel and we're left with $6! \equiv 1 \cdot (1)(1) \cdot 6 \equiv 6 \equiv -1 \bmod 7$.

The conclusion of Wilson's theorem is always false if p is replaced by a composite number n: when n is composite we can't have $(n-1)! \equiv -1 \bmod n$, because if $(n-1)! \equiv -1 \bmod n$ then every integer from 1 to $n-1$ is invertible mod n, which forces n to be prime.[1] Thus we have a primality test:

$$n > 1 \text{ is prime } \textit{if and only if } (n-1)! \equiv -1 \bmod n. \tag{1}$$

At first this might seem superior to the Fermat test, which can often detect composites but doesn't ever prove primality. However, (1) is useless for large n because there is no known fast way of computing $(n-1)!$ mod n, unlike the fast way of computing a^{n-1} mod n for the Fermat test by writing the exponent $n-1$ in base 2 to reduce the exponentiation mod n to repeated squaring mod n.

We now put Wilson's theorem to work.

Theorem 3. *For any prime $p \neq 2$, $-1 \equiv \square \bmod p$ if and only if $p \equiv 1 \bmod 4$.*

[1] In fact, if n is composite then $(n-1)! \equiv 0 \bmod n$ when $n \neq 4$ while $(4-1)! \equiv 2 \bmod 4$.

Proof. First suppose $-1 \equiv \square \bmod p$, say $-1 \equiv x^2 \bmod p$. We don't know much about x, so how can we use x to prove $p \equiv 1 \bmod 4$? Raise both sides to the $(p-1)/2$-power:

$$(-1)^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \bmod p.$$

Since $x \not\equiv 0 \bmod p$ (why?), we know $x^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem since p is prime. Thus

$$(-1)^{(p-1)/2} \equiv 1 \bmod p. \tag{2}$$

The left side is a power of -1, so it is either 1 or -1. Since $p > 2$ we have $-1 \not\equiv 1 \bmod p$, so (2) tells us that $(-1)^{(p-1)/2} = 1$ in $\mathbf{Z}$. Therefore the exponent $(p-1)/2$ is even, say $(p-1)/2 = 2k$ for some $k \in \mathbf{Z}$. Thus $p = 1 + 4k$, so $p \equiv 1 \bmod 4$.

For the converse direction, assume $p \equiv 1 \bmod 4$. To prove $-1 \equiv \square \bmod p$ we will use Wilson's theorem: $-1 \equiv (p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-2)(p-1) \bmod p$. Let's pair together additive inverses mod p: write numbers in the second half of the product as negatives of numbers in the first half, modulo p: $p - k \equiv -k \bmod p$. Then

$$\begin{aligned}
(p-1)! &= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\cdots(p-2)(p-1) \\
&\equiv 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\underbrace{\left(-\left(\frac{p-1}{2}\right)\right)\cdots(-2)(-1)}_{(p-1)/2 \text{ terms}} \bmod p \\
&\equiv (-1)^{(p-1)/2} \cdot 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right)\cdots(2)(1) \bmod p \\
&\equiv (-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2 \bmod p.
\end{aligned}$$

Since $(p-1)! \equiv -1 \bmod p$ by Wilson's, theorem, this congruence says

$$-1 \equiv (-1)^{(p-1)/2}\left(\left(\frac{p-1}{2}\right)!\right)^2 \bmod p. \tag{3}$$

So far this is valid for all odd primes p. If $p \equiv 1 \bmod 4$ then $(p-1)/2$ is even, so $(-1)^{(p-1)/2} = 1$ and the congruence (3) tells us that $-1 \equiv x^2 \bmod p$ where $x = ((p-1)/2)!$. □

Example 4. The first 3 primes that are 1 mod 4 are 5, 13, and 17. We have

$$\left(\frac{5-1}{2}\right)! = 2! \equiv 2 \bmod 5, \quad \left(\frac{13-1}{2}\right)! = 6! = 720 \equiv 5 \bmod 13,$$

and

$$\left(\frac{17-1}{2}\right)! = 8! = 40320 \equiv 13 \bmod 17,$$

and you can verify that these numbers square to $-1 \bmod p$ in each case.

Theorem 3 is not true for odd composites: if n is odd, composite, and positive then the condition $-1 \equiv \square \bmod n$ is *not* equivalent to the condition $n \equiv 1 \bmod 4$. For example, $21 \equiv 1 \bmod 4$ but $-1 \not\equiv \square \bmod 21$. However, one direction is true: if $-1 \equiv \square \bmod n$ then $n \equiv 1 \bmod 4$. Indeed, for each prime factor p of n, $p \neq 2$ and

$$-1 \equiv \square \bmod n \Longrightarrow -1 \equiv \square \bmod p \overset{\text{Thm } 3}{\Longrightarrow} p \equiv 1 \bmod 4.$$

Since n is the product of its prime factors, we get $n \equiv 1 \bmod 4$.

Appendix A. Comments on Wilson's Theorem

Wilson's theorem is named after John Wilson, who conjectured the result as a student. His conjecture was published in the book *Meditationes Algebraicae* written (in Latin) by his teacher Edward Waring in 1770. The page containing the statement of Wilson's theorem can be found in [1, Figure 2] (see the paragraph that begins "Sit n numerus primus"). Lower down on the same page is the following claim by Waring, which shows how limited his perspective was on number theory: "Proofs of propositions of this kind are made more difficult by the fact that one can't imagine a convenient notation for prime numbers." Other mathematicians were more imaginative than Waring: the first proof of Wilson's theorem was given by Lagrange [3] in 1771, using polynomials mod p, and Lagrange also observed that the congruence $(n-1)! \equiv -1 \bmod n$ only holds for prime n. In 1801, Gauss [2, Article 77] proved Wilson's theorem by the argument we gave that pairs together multiplicative inverses modulo p, and he criticized Waring's comment about the lack of notation for primes, saying [2, Article 76] "In our opinion, truths of this kind should be drawn from notions rather than from notations." Gauss also proved a generalization of Wilson's theorem to all moduli $m \geq 2$ using the product of the units mod m:

$$\prod_{a \in (\mathbf{Z}/(m))^\times} a \equiv \begin{cases} -1 \bmod m, & \text{if } x^2 \equiv 1 \bmod m \text{ has at most two solutions,} \\ 1 \bmod m, & \text{if } x^2 \equiv 1 \bmod m \text{ has more than two solutions.} \end{cases}$$

The first condition occurs not only when m is prime. It also happens when m is 4, an odd prime power, and twice an odd prime power.

While $(p-1)! \equiv -1 \bmod p$ for all primes p, it is rare that $(p-1)! \equiv -1 \bmod p^2$. Such p are called *Wilson primes* and the only examples up to 10^{13} are 5, 13, and 563. Probabilistic heuristics suggest there should be infinitely many such primes, and also that they should be extremely rare. Concerning the infinitude of Wilson primes, Harry Vandiver [4] once wrote "This question seems to me to be of such a character that if I should come to life any time after my death and some mathematician were to tell me that it had been definitely settled, I think I would immediately drop dead again."

References

[1] G. L. Alexanderson, L. F. Klosinski, "About the cover: Waring's problems," *Bull. Amer. Math. Soc.* **55** (2018), 375–379. Online at https://www.ams.org/journals/bull/2018-55-03/S0273-0979-2018-01629-7/.

[2] C. F. Gauss, *Disquisitiones Arithmeticae* (English edition), Springer-Verlag, 1986.

[3] J–L. Lagrange, "Démonstration d'un théorème nouveau concernant les nombres premiers," *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres*, Berlin (1771), 425–438. Online at https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f426.

[4] H. S. Vandiver, "Divisibility Problems in Number Theory," *Scripta Mathematica* **21** (1955), 15–19. Online at https://books.google.com/books?id=0-Y4AAAAIAAJ&source=gbs_book_other_versions.